Basic Axioms and Examples

Note 1

Given a set G, {{c2: a binary operation $\star$ on G}} is {{c1: a function

$$\star : G \times G \to G.$$

}}

Note 2

Given a binary operation $\star$ on a set G, for any $a, b \in G$ we shall write {{c2: $a \star b$}} for {{c1: $\star(a, b)$.}}

Note 3

A binary operation $\star$ on a set G is {{c2: associative}} if {{c1: for all $a, b, c \in G$ we have

$$a \star (b \star c) = (a \star b) \star c.$$

}}

Note 4

If $\star$ is a binary operation on a set G we say elements a and b of G {{c1: commute}} if {{c2:

$$a \star b = b \star a.$$

}}

Note 5

A binary operation $\star$ on a set G is {{c2: commutative}} if {{c1: for all $a, b \in G$ we have
$$a \star b = b \star a.$$

}}

Note 6

Suppose that $\star$ is a binary operation on a set G and $H \subseteq G$. If {{c2: the restriction of $\star$ to H is a binary operation on H,}} then H is said to be {{c1: closed under $\star$.}}

Note 7

{{c3::A group}} is {{c2::an ordered pair $(G, \star)$}} where {{c1::G is a set and $\star$ is a binary operation on G}} satisfying {{c4::the group axioms.}}

Note 8

How many axiom are there in the definition of a group $(G, \star)$?

❚ Three.

Note 9

What is the first axiom from the definition of a group $(G, \star)$?

❚ $\star$ is associative.

Note 10

Given a binary operation $\star$ on a set G, {{c3::an element $e \in G$}} is called {{c2::an identity of G}} if {{c1::for all $a \in G$ we have

$$a \star e = e \star a = a.$$

}}

Note 11

What is the second axiom from the definition of a group $(G, \star)$?

❚ There exists an identity of G.

Note 12

Given a binary operation $\star$ on a set G and $a \in G$, {{c3::an element $\tilde{a} \in G$}} is called {{c2::an inverse of a}} if {{c1::

$$a \star \tilde{a} = \tilde{a} \star a = e.$$

}}

Note 13

d840b7b910d740f3bea231c74feba51c

Given a binary operation $\star$ on a set G and $a \in G$, {{c2: an inverse of a}} is usually denoted {{c1: a^{-1}.}}

Note 14

c4c56a11c6f746b3ae287ee386b4e12b

What is the third axiom from the definition of a group $(G, \star)$?

▎ For all $a \in G$ there exists a^{-1}.

Note 15

be05e23d350d4f49a65602b65045f888

A group $(G, \star)$ is called {{c2: abelian}} if {{c1: $\star$ is commutative.}}

Note 16

978f23382d594a28a3de168b7f661c30

We shall say G is {{c2: a group under $\star$}} if {{c1: $(G, \star)$ is a group.}}

Note 17

497f01593d7f4ffabb546b455788b354

We shall say a set G is {{c2: a group}} if {{c1: G is a group under an operation that is clear from the context.}}

Note 18

61ea2504ca474fe4aae902eb1965576c

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are {{c2: groups}} under {{c1: $+$.}}

Note 19

84b6a231d3934ab3b4f63226549a9589

$\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0\}$ are {{c2: groups}} under {{c1: $\times$.}}

Note 20

3051cd354f5040e2bdf0809e005635ed

$\mathbb{Q}^{+}, \mathbb{R}^{+}$ are {{c2: groups}} under {{c1: $\times$.}}

Note 21

21f924e833cd4e0bbae5f4588dff47b5

Is $\mathbb{Z} - \{0\}$ a group under $\times$?

▎ No. (There is no inverse.)

Note 22

Let V be a vector space. Then V is {{c2::a group}} under {{c1::$+$.}}

Note 23

Let $n \in \mathbb{Z}^+$. Then {{c3::$\mathbb{Z}/n\mathbb{Z}$}} is {{c2::a group}} under {{c1::addition}} of residue classes.

Note 24

Let $n \in \mathbb{Z}^+$. Then {{c3::$(\mathbb{Z}/n\mathbb{Z})^\times$}} is {{c2::a group}} under {{c1::multiplication}} of residue classes.

Note 25

If $(A, \star)$ and $(B, \diamond)$ are {{c4::groups,}} then the group {{c2::$A \times B$,}} whose operation is {{c1::defined componentwise:

$$(a, b)(c, d) = (a \star c, b \diamond d),$$

}} is called {{c3::the direct product of the two groups.}}

Note 26

If $(G, \star)$ is a group, then {{c2::the identity of G}} is {{c1::unique.}}

Note 27

If $(G, \star)$ is a group, then the identity of G is unique. What is the key idea in the proof?

▌ Consider the product of two arbitrary identities.

Note 28

If $(G, \star)$ is a group, then for every $a \in G$, {{c2::a^{-1}}} is {{c1::uniquely determined.}}

Note 29

If $(G, \star)$ is a group, then for every $a \in G$, a^{-1} is uniquely determined. What is the key idea in the proof?

▎ Multiply an inverse on the right by $a \star a^{-1}$.

Note 30

If $(G, \star)$ is a group and $a \in G$, then

$$(a^{-1})^{-1} = {}_{\{\{c1::}a.\}\}}$$

Note 31

If $(G, \star)$ is a group and $a, b \in G$, then

$$\{\{c2::}(a \star b)^{-1}{}_{\}\}} = {}_{\{\{c1::}}(b^{-1}) \star (a^{-1}).\}\}$$

Note 32

If $(G, \star)$ is a group and $a_1, \ldots, a_n \in G$, then the value of

$$a_1 \star \cdots \star a_n$$

is {{c2::independent}} of {{c1::how the expression is bracketed.}}

«{{c3::The generalized associative law}}»

Note 33

What is the key idea in the proof of the generalized associative law for a group $(G, \star)$?

▎ By induction.

Note 34

Henceforth our abstract groups G, H, *etc.* will always be written with the operation as {{c1::$\cdot$.}}

Note 35

Henceforth for an abstract group G (operation $\cdot$) an expression $a \cdot b$ will always be written as $ab.$

Note 36

Henceforth for an abstract group G (operation $\cdot$) we denote the identity of G by $1.$

Note 37

For any group G and $x \in G$ and $n \in \mathbb{Z}^+$ we shall denote by x^n the product

$$\underbrace{xx \cdots x}_{n \text{ terms}} .$$

Note 38

For any group G and $x \in G$ and $n \in \mathbb{Z}^+$ we shall denote by x^{-n} the product

$$\underbrace{x^{-1}x^{-1} \cdots x^{-1}}_{n \text{ terms}} .$$

Note 39

For any group G and $x \in G,$ let $x^0 \stackrel{\text{def}}{=} 1$, the identity of $G.$

Note 40

Let G be a group and let $a, u, v \in G$. Then $au = av$ if and only if $u = v.$

«Cancellation rule»

Note 41

For G a group and $x \in G$ define the order of x to be the smallest positive integer n such that

$$x^n = 1.$$

Note 42

For G a group and $x \in G$, if no positive power of x is the identity, the order of x is defined to be infinity.

Note 43

For G a group and $x \in G$, denote the order of x by $|x|$.

Note 44

For G a group and $x \in G$, if the order of x is an integer n, x is said to be of order n.

Note 45

For G a group and $x \in G$, if the order of x is infinite, x is said to be of infinite order.

Note 46

An element of a group has order 1 if and only if it is the identity.

Note 47

Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with $g_1 = 1$. The multiplication table or group table of G is the matrix

$$\left[g_i g_j \right] \sim n \times n.$$

Note 48

Let $G = \{x \in \mathbb{R} \mid x \in [0, 1)\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$. Then the group $(G, \star)$ is called the real numbers mod 1.

Note 49

Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Then the group $(G, +)$ is called the group of roots of unity in $\mathbb{C}$.

Note 50

A finite group is abelian if and only if its group table is a symmetric matrix.

Note 51

Let G a group and $x \in G$ and $a, b \in \mathbb{Z}$. Then $x^{a+b} = x^a x^b$.

Note 52

Let G a group and $x \in G$. Then $|x^{-1}| = |x|$.

Note 53

Let G a group and $x, g \in G$. Then $|g^{-1}xg| = |x|$.

Note 54

Let G a group and $a, b \in G$. Then $|ba| = |ab|$.

Note 55

Let G a group, $x \in G$, $|x| = n < \infty$ and $s \in \mathbb{Z}$. Then $x^s = 1$ if and only if $n \mid s$.

Note 56

Let G a group, $x \in G$, $|x| = n < \infty$ and $s \in \mathbb{Z}$. Then

$$|x^s| = \frac{n}{(n, s)}.$$

Note 57

Let G a group, $x \in G$, $|x| = n < \infty$ and $s \in \mathbb{Z}$. Then $|x^s| = \frac{n}{(n,s)}$.
What is the key idea in the proof?

▎ $(x^s)^k = 1$ if and only if $n \mid sk$.

Note 58

Let G a group, $a \in G$. If $x^2 = 1$ for all $x \in G$ then

$$a^{-1} = {\{\{c1::a.\}\}}$$

Note 59

Let G a group. If {{c3::a and b are commuting elements of G}} then
{{c2::$(ab)^n$}} $=$ {{c1::$a^n b^n$}}.

Note 60

Let G a group. If $x^2 = 1$ for all $x \in G$ then G is {{c1::abelian.}}

Note 61

Let G a group. If $x^2 = 1$ for all $x \in G$ then G is abelian. What is
the key idea in the proof?

▎ $1 = (ab)^2$ and multiply by a on the left and by b on the right.

Note 62

Let $(G, \star)$ be a group and {{c4::$H \subseteq G$.}} If {{c2::H is a group under the
operation $\star$ restricted to H}} then {{c3::H}} is called {{c1::a subgroup of
G.}}

Note 63

Let G a group and {{c3::$x \in G$.}} Then {{c2::the subgroup $\{x^n \mid n \in \mathbb{Z}\}$
of G}} is called {{c1::the cyclic subgroup of G generated by x.}}

Note 64

7d1e317bc7c64c538d09a6fd6c2e2011

Let A and B be groups. Then $A \times B$ is {{c3: abelian}} {{c2: if and only if}} {{c1: both A and B are abelian.}}

Note 65

c048d6c9ce83411c94e040e5991b3524

Let A and B be groups, $(a, b) \in A \times B$. Then the order of (a, b) is {{c1: the least common multiple of $|a|$ and $|b|$.}}

Note 66

de71dcf7adc64bcd9b53502c90a0cefa

Let A and B be groups, $(a, b) \in A \times B$. Then

$$(a, b)^k = {{c1: (a^k, b^k)}}$$

for all $k \in$ {{c2: $\mathbb{Z}$}}.

Note 67

e672cc6907124507a4fd998675844d02

Let A and B be groups, $(a, b) \in A \times B$. Then the order of (a, b) is the least common multiple of $|a|$ and $|b|$. What is the key idea in the proof?

$(a, b)^k = (a^k, b^k)$.

Note 68

e6f9e981e45d4f55a3aafa3eb6d77ef1

Any finite group of {{c2: even}} order contains an element of order {{c1: 2.}}

Note 69

d13862b410194166829309d8ea4880a6

Any finite group of even order contains an element of order 2. What is the key idea in the proof?

Show that the set $\{g \in G \mid g \neq g^{-1}\}$ has an even number of elements.

Note 70

Let G a group, $x \in G$ and $|x| = n < \infty$. Then the elements {{c2::

$$1, x, x^2, \ldots, x^{n-1}$$

}} {{c1::are distinct.}}

Note 71

Let G a group, $x \in G$ and $|x| < \infty$. Then $|x|$ {{c2:: $\leq$ }}{{c1:: $|G|$ }}.

Note 72

Let G a group, $x \in G$ and $|x| < \infty$. Then $|x| \leq |G|$. What is the key idea in the proof?

The elements $1, x, \ldots, x^{n-1}$ are the only powers of x.

Note 73

Let G a group, $x \in G$ and $|x| = \infty$. Then the elements {{c2::

$$x^n, n \in \mathbb{Z}$$

}} {{c1::are distinct.}}

Dihedral Groups

Note 1

A symmetry of a regular n-gon is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it.

Note 2

Each symmetry of a regular n-gon can be described uniquely by the corresponding permutation of $\{1, 2, \ldots, n\}$, representing the permutation of the vertices.

Note 3

Given $n \in \mathbb{Z}^+$ and $n \geq 3$, let D_{2n} be the set of symmetries of a regular n-gon.

Note 4

Given $n \in \mathbb{Z}^+, n \geq 3$ and $s, t \in D_{2n}$, the product st is defined to be the symmetry obtained by first applying t then s to the n-gon.

Note 5

Given $n \in \mathbb{Z}^+$ and $n \geq 3$, the group D_{2n} is called the dihedral group of order $2n$.

Note 6

Given $n \in \mathbb{Z}^+$ and $n \geq 3$,

$$|D_{2n}| = 2n.$$

Note 7

Given $n \in \mathbb{Z}^+$ and $n \geq 3$, $|D_{2n}| = 2n$. What is the key idea in the proof?

> Every symmetry is uniquely determined by how it affects some two adjacent vertices.

Note 8

For convenience, the regular n-gon viewed in D_{2n} is fixed {{c1:: centered at the origin.}}

Note 9

For convenience, the vertices of the regular n-gon viewed in D_{2n} are labeled {{c1:: consecutively from 1 to n in a clockwise manner.}}

Note 10

In the context of the D_{2n} group, let {{c2::r}} be {{c1:: the rotation clockwise about the origin through $2\pi/n$ radian.}}

Note 11

In the context of the D_{2n} group, let {{c2::s}} be {{c1:: the reflection about the line of symmetry through vertex 1 and the origin.}}

Note 12

In the context of the D_{2n} group, is it possible that $s = r^i$ for some i?

▮ No.

Note 13

In the context of the D_{2n} group, is it possible that $sr^i = sr^j$ for some $i \not\equiv j \pmod{n}$?

▌ No.

Note 14

Each element of D_{2n} can be written {{c2::uniquely}} in the form {{c1:: $s^k r^i$ for some $k = 0$ or 1 and $0 \leq i \leq n - 1$.}}

Note 15

In the context of the D_{2n} group,

$$r^i s = {{c1::sr^{-i}, }} \text{ for } {{c2::all } 0 \leq i \leq n}}.$$

Note 16

In the context of the D_{2n} group,

$$r^i s = sr^{-i}, \text{ for all } 0 \leq i \leq n.$$

What is the key idea in the proof?

▌ $rs = sr^{-1}$ and by induction.

Note 17

{{c3::A subset S of elements}} of a group G with the property that {{c1::every element of G can be written as a (finite) product of elements of S and their inverses}} is called {{c2::a set of generators of G.}}

Note 18

If S is {{c2::a set of generators}} of a group G, we shall write {{c1::

$$G = \langle S \rangle.$$

}}

Note 19

If S is {{c2::a set of generators}} of a group G, we shall say G is {{c1:: generated by S.}}

Note 20

In terms of generators, the group $D_{2n} = \langle r, s \rangle$.

Note 21

In a finite group G a set S generates G if every element of G is a finite product of elements of S.

Note 22

In the D_{2n} group, the relations $r^n = 1$, $s^2 = 1$ and $rs = sr^{-1}$ have the additional property that any any other relation between elements of the group may be derived from these three.

Note 23

In the D_{2n} group, the relations $r^n = 1$, $s^2 = 1$ and $rs = sr^{-1}$ have the additional property that any any other relation between elements of the group may be derived from these three. What is the key idea in the proof?

> We can determine exactly when two group elements are equal by using only these three relations.

Note 24

Any equations in a general group G that the generators satisfy are called relations in G.

Note 25

Let G be a group. If G is generated by a subset S and there is some collection of relations such that any relation among the elements of S can be deduced from these, we shall call these generators and relations a presentation of G.

Note 26

Let G be a group. If a subset S and a collection of relations $R_1, \ldots, R_m$ form a presentation of G, we shall write

$$G = \langle S \mid R_1, \ldots, R_m \rangle.$$

Note 27

One presentation for the dihedral group D_{2n} is

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, \ rs = sr^{-1} \rangle.$$

Note 28

If $n = 2k$ is even and $n \geq 4$ then r^k is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}.